Copy to DD (CSA) 2/9

p. 3 French
p. 4 Russian Sig Int.

15(I)

TOP SECRET "U"

TICOM/I-75

GSI(S), 21 Army Group has supplied the attached interrogation reports on German Field Sigint personnel carried out at BUFFER. (Date of covering memo. 18 Aug.'45)

POW's handled and dates were as follows:-

Ltn. August SCHROEDER of Tel. Bau Rgt. RANDEWIG (11 Aug. '45)

Ltn. STARKE (NNAK on Russian front) (11 Aug. '45)

Obgefr. HEUDORF (NAA 8 - 3Pz Army) (11 Aug. '45)

Hptm. HOLETZKO (14/ln. Rgt. 1 = 1/Ln. Rgt. 353) (11 Aug. '45)

There are also technical notes on Russian codes and cyphers, consolidated from the various interrogations carried out on the 11 Aug. '45.

TICOM
28 August '45

Copy No. 11
No. of pp. 12

Distribution:

British
1 Director
2 D.D.3
3 D.D.4
4 D.D.(N.S.)
5 D.D.(M.W.)
6 D.D.(A.S.)
7-8 A.D.(C.C.R.)(2)
9 Lt.Col. Leathem

U.S.
26-27 OP20-G(2)(via Lt. Pendergrass)
28 G-2(via Lt.Col. Hilles)
29-30 S.S.A.(2)(via Major Seaman)
31 Director S.I.D. USFET (via Lt.Col. Johnson)

TICOM
10 Chairman
11-12 S.A.C.(2)
13 Cdr. Bacon
14 Cdr. Mackenzie
15 Cdr. Tandy
16 Lt.Col. Johnson
17 Lt.Col. Lewis Powell
18 Lt.Cdr. Manson
19 Major Morgan
20 Major Seaman
21 Lt. Vance
22 Capt. Cowan
23 Lt. Fehl
24-25 Ticom files(2)

Additional
32-34 Lt.Col. Pritchard(3)

21 A Gp/IS/INT/359/525
18 Aug 45

1. Enclosed reports on the first series of interrogations on Field Sig Int Personnel carried out at BUFFER interrogation camp.
2. Please let us know if any points of particular interest arise from these reports and we will endeavour to follow them up.
3. Please acknowledge receipt on attached substitute A.F.A16.

? Major G.S.
for Lieut.-Colonel, G.S.

G.S.I(s),
H.Q., 21 Army Group.
Ext 3050.

/HC

Report on the Interrogation of Ltn AUGUST SCHROEDER 11 Aug 45.

1. PRELIMINARY REMARKS.

Home Address:- BIELEFELD, Steinmetzstr. 1 (British Zone).

Age 31 years. Married. Business man by profession.

PW had 9 years military experience, mostly in Sig Int. He showed some knowledge of general Sig Int problems, as, for some time, he had handled policy matters at AOK9. His long military career is best shown in tabular form:-

Date	Unit
Oct 36 - Dec 37	Nachr Abt 6 in BIELEFELD.
Dec 37 - Sep 38	Condor Legion in SPAIN.
Sep 38 - Oct 38	Nachr Abt 6 BIELEFELD then discharged.
Oct 39 - Oct 40	Special OKW/OKH Sig Int unit in SPAIN.
Nov 40 - Apr 41	OKW/Chi - Monitoring FRENCH external wireless comms for the Armistice Commission
May 41 - Oct 41	Nachr Ers Komp 254 in LINGEN and NAMUR.
Oct 41 - Feb 42	Nachr Abt 6, committed on CENTRAL RUSSIAN front.
Feb 42 - Dec 43	Armeenachr Rgt 511 on CENTRAL RUSSIAN front. PW acted as adviser on Sig Int matters at AOK9.
Dec 43 - May 44	In hospital.
May 44 - Apr 45	Nachr Abt 6 in BIELEFELD.
Apr 45 -	Tel Bau Rgt RANDEWICH.

2. WITH THE CONDOR LEGION IN SPAIN.

The experimental Sig Int unit in SPAIN, known as "IMKER)WOLM" and later "IMKER-HORCH", combined strategical and tactical intercept. Although the main intercept, W/T'I' and code breaking effort was concentrated at the Condor Legion H.Q., detachments were occasionally sent up to the front line. The REPUBLICAN Army maintained a high level of wireless discipline and worked mostly Netz. Call-signs - three letter - changed at the beginning of each month and later, weekly. Five figure tfc predominated and was almost completely readable, thanks to a REPUBLICAN Army offr who handed over the key before breaking had been attempted.

3. MONITORING OF FRENCH LINKS.

During the period before and after the collapse of FRANCE,

PW was with a special OKW/OKH org in SPAIN, monitoring the FRENCH colonial wireless networks in N.W. AFRICA, the SAHARA and BELGIAN CONGO. The army sta operated near MADRID, the Air Force at BARCELONA and the Navy in SEVILLE. Both 5-fig and clear msgs were taken; the 5-fig tfc being forwarded to OKW/Chi. Latterly, particular importance was given to the wireless link BRAZZAVILLE - LEOPOLDVILLE between General de GAULLE and the BELGIAN Governor RYCKMANNS. The Italians indulged in similar activities from a sta in MADRID.

While at OKW/Chi, PW was engaged in monitoring the FRENCH external wireless links, for which task the fixed intercept stas at LAUFF and TREUENBRIETZEN were responsible. Breaches of the regulations were reported immediately by OKW/Chi to the Armistice Commission in WIESBADEN. PW cited a case of tfc from PARIS for BEIRUT, being routed via ONGAR.

4. GERMAN SIG INT ORG IN RUSSIA.

In 1939, to the three secs of a GERMAN Sigs Coy was added a fourth, known as the Nachrichtennahaufklaerungszug or NAZ. Its strength was 1 offr 3 NCO's and 30 men, equipped with 4 - 6 Torn Empf b. or Horchempf u. With tactical interception as their object, these secs only achieved success shortly before the end of the campaign in FRANCE. The O's.C. of the signal units to which they were attached had little interest in or understanding of Sig Int. On the Russian front, PW's own unit (the NAZ of Nachr Abt 6) achieved considerable success in the KALININ - RSHEW area when it changed to taking R/T in place of W/T. Inf regt links down to coy provided a very clear picture of enemy dispositions and intentions. On the strength of this success, PW was appointed adviser in Sig Int matters at AOK9.

An attempt to equate the work of the various NAZ by forming them into gps was thwarted by an OKH order of Apr 42 which created a Nachrichtennahaufklaerungskompanie at army level out of the disbanded NAZ's. W/T'I' and code breaking were carried out near the army H.Q. from raw material provided by three intercept secs detached to corps. A D/F sec with 3 short range D/F's operated as far forward as bns and even outside the army area. The coy also had a line-tapping sec (Drahtaufklaerungszug) equipped with 2 Lauschempfaenger 40 or 42 and later the Lauschempfaenger "klein". This sec, operating from an inf coy, could only go out in summer, as in winter the return journey through the snow presented considerable problems. During the retreat, lines or search-earths were left ready for tapping PW stated that such secs had considerable success and infm of local attacks, arty concentrations etc normally reached the inf coy in time.

PW felt very strongly that the NAK's at army level were wasted owing to the delay in communicating vital infm to the forward troops. In consequence it was proposed that detachments should be allotted to divs. A conference on this subject at OKH in Dec 43 came to no conclusions and AOK9 took independent action in creating its own Nachrichtennahaufklaerungstrupps which some months later were recognised by OKH. A NNAT in charge of an NCO had 2 interpreters and 8 men operating 2 Torn Empf b.

5. RUSSIAN SETS.

Forward of div PW knew only of an inf set with range of 15 kms on W/T and 5 - 6 kms on R/T. The morse-key was a rubber knob built into the top of the set and produced somewhat extended signals. For R/T, a throat microphone was used.

Partisans were equipped with special short wave sets whose

range was barely half a mile.

P.W. suspected that American sets were sometimes used on his front.

6. Freqs and Call Signs

In the experience of thd P.W., links forward of div worked in the 2200 - 3900 Kc/s band, concentrating between 3100 and 3400 Kc/s. Freqs were spaced at intervals of 25 Kc/s corresponding to a single graduation on the dials of the sets. The traffic appeared around 1200 Kc/s. Call signs of 3 or 4 letters were employed on W/T, while for R/T 4 figure call signs predominated. P.W. had only known R/T code names on air-to-ground links.

In the early days, freqs changed weekly, but later a daily change of freqs and call signs took place at midnight.

P.W. recognised that these conditions were at variance with those obtaining on other fronts and emphasised that they applied to the 5 and 43 RUSSIAN Armies on the CENTRAL front.

7. Security

The RUSSIANS introduced control stations for monitoring their networks; these stations would sometimes break in on activity. In spite of this, coy and sec comds regarded R/T as an ordinary telephone and spoke very freely. Code words were rarely in evidence and remained fairly constant; examples were box = tk, peas = amn, rain = attack, cow = rocket-projector. Very many private conversations were heard and these gave useful indications of enemy morale. Although 2 figure traffic was never very difficult to read, much assistance was gained from security breaches on the part of RUSSIAN operators. On the other hand, the RUSSIANS reached a high standard of sending in W/T. This, the P.W. attributed to good pre-military training. In KALININ he himself had seen a school for youths with 200 training keys. With some bitterness, the P.W. referred to the capture of Hptm SEEBOHM's unit in the EL ALEMEIN area and the subsequent disappearance of the informative first group in RUSSIAN 5 figure messages. From operators' chat in Jan 43, it appeared that an ANGLO-AMERICAN delegation was visiting the CENTRAL RUSSIAN front. Equally, the arrival of high RUSSIAN Officers was often disclosed in private conversations, as occasionally were dates of impending attacks. On partisan networks, particularly good operators were employed. D/F was well-nigh impossible, owing to the short duration of activity and hourly-changing freqs. To the P.W's knowledge, the detachments which were formed in the winter of 43 to trace this activity met with no success.

8. RUSSIAN Sig Int

Towards the end of 43, it first became noticeable that the RUSSIANS had committed intercept detachments in forward areas. P.W. had also captured a document addressed to the fifth RUSSIAN Army, drawing its attention to the importance of Sig Int.

A female RUSSIAN operator, attached to a GERMAN Sig Int unit in AOK 9 as a decoder, stated that the RUSSIAN organisation was built up on GERMAN lines. GERMAN deserters, who had placed themselves at the disposal of the FREE GERMAN COMMITTEE, were largely engaged on Sig Int. A RUSSIAN code message taken in the BELIJ pocket began "Our intercept service has just taken and decoded the following GERMAN message.....". The text of the message followed.

Report on the Interrogation of Ltn STARKE 11 Aug 45.

1. PRELIMINARY REMARKS.

Home Address:- FALKENBERG/ELSTER, Torgauerstr. 18. (Russian Zone).

Age 35 years. Married. Business man by profession.

PW served as a W/T operator in Div Sigs from the outbreak of the war until May 42 when he transferred to a Nachrichtennahaufklaerungskompanie (NNAK) on the Central Russian front. There, he had experience as an intercept operator and later, on the W'I' side, as a specialist in D/F and W/T 'I' matters. PW proved most cooperative, but his knowledge was limited to his own part of the front and his memory failed him on certain details.

2. GERMAN SIG INT ORG IN THE FIELD.

The normal Sig Int unit at army level was the Nachrichtenaufklaerungsabteilung (NAA) consisting of two coys: a Fernaufklaerungskompanie (FAK), primarily concerned with the comd nets down to div level, and a Nahaufklaerungskompanie (NAK) responsible for links from div down to bn level. In practice, the two coys worked in close cooperation and the staff of the NAA, its W'I' sec and the W'I' secs of the two coys would always be located together in the vicinity of Army H.Q.

Each NAK had two Nachrichtenaufklaerungszuege (NAZ) or secs operating forward, sometimes at corps and one always with the assault corps.

A NAZ comprised 1 offr, 6 NCO's, 6 interpreters and from 15 to 20 intercept operators. At its disposal it had up to 10 sets (6 Horchempfaenger b and 4 Torn. Empfaenger b) and 6 to 8 D/F sets. In important sectors a line-tapping unit would be sent forward from the NAK and put under comd of the NAZ.

3. RUSSIAN SETS.

The only Russian set of which the PW had detailed knowledge was the RBW2, the most common in his sector from div down to bn. He had seen a captured model and gave the following description:- Transmitter and receiver were housed in one container, while a second held the accessories, batteries etc. The whole weighed about 45 lbs and was carried by one man. It had a freq range of 750 - 3050 kcs graduated into units of 25 kcs on both transmitter and receiver. The set was used mainly for R/T (range up to 10 kms), although W/T (up to 25 kms) came up at night or under bad reception conditions.

4. FREQS AND CALL-SIGNS.

a) FORWARD OF DIV. On inf and arty links, where the RBW2 was in use, most activity lay between 1300 and 2300 kcs with the peak band 1750 - 2200 kcs. Freqs and call-signs changed at least three times each month but not at regular intervals. Code-names of the type TEREK, KUBAN, ODESSA, OPTIKA which appeared in R/T were abbreviated to the first three letters for W/T e.g. TER, KUB etc. PW knew nothing of the sets employed by armd or air force fmns but stated that activity was always in the 3000 - 4800 kcs range. Tks resorted to wireless only after the battle had been joined.

b) COMD LINKS DOWN TO DIV. Almost exclusively W/T with main

activity between 1950 and 2250 kcs. Freqs changed three times monthly, while call-signs changed daily. Call-signs were made up of two or three symbols, mostly mixed figures and letters. By Mar 44 the complete system had been worked out and PW received thoroughly reliable predictions for all known stas. The system had been resolved statistically. Each known sta was given a number which each day was entered on a chart of all possible call-signs. The chart had a separate sheet for every possible first symbol of the call-signs with the second and third symbols as coordinates of a square. Over time, patterns were discovered and prediction became possible. PW was not clear what form the patterns took, as he had never worked on the system. He merely received a list of call-signs for each sta number. In Jul 44, after a long wireless silence before the summer offensive, the system changed. PW had little idea how the new system worked but he thought that, by the end of the war, good progress had been made in breaking it down.

5. IDENTIFICATION OF NEW GPS.

a) Number of stas on the gp.
b) D/F (Org roughly the same as our own).
c) Type of working: R/T or W/T.
d) Type of tfc. e.g. 5-fig cipher would place gp above div level.
e) If 5-fig. cipher were used, careful statistical records of the indicator groups, serial numbers etc. gave an additional indication of the fmn. (see Tech notes on Codes and Ciphers).
f) The Russians had a habit of giving numbers to their offrs, the highest ranks having the highest numbers. Msgs might be prefixed "dla (for) 27" and be signed "25". From observation of the direction of tfc over a day, it was possible to determine the senior sta on a net.

6. CODES AND CIPHERS.

PW had experience of 2-fig, 3-fig, 4-fig, 5-fig tfc, and, more occasionally, mixed fig and letter. Given depth of tfc, all codes were readable, except the 5-fig which PW regarded as unbreakable. He himself had little knowledge of breaking methods but gave details of the codes themselves. These have been incorporated in the "Tech Notes on Codes and Ciphers"

7. CONTENTS OF MSGS.

Most readable tfc consisted of routines such as tk, amn and ration states. For detecting movements and rfts, which were seldom mentioned in tfc, D/F proved invaluable.

8. PROCEDURE SIGNALS.

Mostly amateur or international.

9. CONCLUSION.

Details given above apply only to the first WHITE RUSSIAN front during the period May 42 until the end of the war. PW described Sig Int results on this front as outstandingly successful, in spite of the periodic improvements in Russian security.

Report on the Interrogation of Obgefr. HEUDORF 11 Aug 45.

1. PRELIMINARY REMARKS.

Home address:- DAHLBRUCH/Kreis SIEGEN i.W.
Age: 31 years. Married. Occupation: Confidential clerk in the firm of SIEMAG in DAHLBRUCH.

PW had been trained as a W/T operator and later as an intercept operator. He spent 16 months on the RUSSIAN front with the Fernaufklaerungskompanie (FAK) of Nachrichtenaufklaerungsabteilung (NAA) 8 which was attached to 3 Pz Army. NAA8 belonged to Nachrichtenaufklaerungsregiment (NAR) 2, the Sig Int unit of Army Group VISTULA. Of his 16 months, PW spent one year on the Sigs side and only 4 months with the W.I. sec. With such short experience, PW could give very little first-hand information, although he knew something of the RUSSIAN W/T links above div.

2. GERMAN SIG INT ORG IN RUSSIA.

The original intention of close cooperation between the FAK and NAK of an Abteilung was not fulfilled in NAA8, and in practice the two coys worked independently. A staff, some 25 strong, coordinated the results of the two branches and compiled a daily report for G(Int) at 3 Pz Army and for NAR2 (the Army Group Sig Int unit).

A FAK had 2 offrs (an O.C. coy and an offr i/c W.I.) and some 160 NCOs and men. The labour was divided roughly as follows:-

	Section		Strength
i)	Operating sec (manning approx 20 sets)		64
ii)	D/F sec (5 dets)		30
iii)	Comns sec		18
iv)	W.I.sec a) D/F 4		22
	b) W/T'I' 10		
	c) Breakers & Decoders 8		
v)	Adm sec		26

The org of work was very similar to our own, even down to the standardised requests for bearings.

3. RUSSIAN COMD NETS DOWN TO DIV.

a) FREQS AND CALL-SIGNS. Activity occurred mainly in the 1800 - 2600 kcs band with outside limits 1400 - 3600 kcs. Freqs would remain constant for long periods, sometimes up to a month. There were exceptions such as Eng units whose freqs changed every 3 days.

Call-signs were almost always of the 3 symbol type (letters or mixed figure and letter). If a unit were split, e.g. tac and main HQ, then number suffixes would be added to the basic call-sign e.g. iNR and iNR1.

Until Jul 44, the call-sign system was well known to the GERMANS and predictions reliable. The 1944 summer offensive, however, brought a change of system. By the end of hostilities, the GERMANS had made good progress in solving this new system, but its workings were unknown to PW.

b) CODES AND CIPHERS. 4-Fig tfc had on occasion provided some difficulty. On the other hand PW recalled an Eng unit in Mar and Apr 45 whose 4-Fig msgs were read currently. Tk states

proved particularly useful as a fixed proforma was used, and simple arithmetic would confirm the accuracy of the idents.

5-Fig, although unbreakable, was of considerable value to W/T'I' (See Tech Notes on Codes and Ciphers).

PW had known 2 and 3 fig codes only to be used for adm matters and thought them very easy to break.

c) PROCEDURE SIGS. Although the RUSSIANS, in common with the general improvement in their wireless working, gradually abandoned "native" procedure signals in favour of the international Q and Z codes, several of the old ones survived e.g. GUHOR = I cannot hear you. NIL = I have nothing for you.

d) D/F. Experience proved the LM-Peiler with a range up to 3750 kcs to be the best eqpt. D/F dets were committed 5 - 20 kms behind the front and covered a range of up to 160 kms. During the periods of wireless silence which the RUSSIANS developed towards the end of the war, D/F of the occasional tuning was the only source of Sig Int to the FAK.

4. CONCLUSION.

PW was particularly impressed by the 7 week's wireless silence which preceded the RUSSIAN offensive in Jul 44 and the complete change of systems which followed it. From that time, Sig Int in itself became very difficult and the constant retreat made matters worse.

Report on the Interrogation of Hptm HOLETZKO 11 Aug 45.

1. PRELIMINARY REMARKS

Home Address:- BOBREK-KARF, Kreis BEUTHEN, Brunnenstr.1. (Russian Zone).

Age 26 years. Single.

After completing his Abitur, P.W. left school to go straight into the Forces. He had served almost continuously in Sig Int since Sep 40, in the following units:-

Date	Unit
Sep 40 - Nov 40	9/Ln Rgt Ob. d.L. (FRANCE)
Nov 40 - Jul 42	4/Ln Rgt 38
Sep 42 - Aug 43	9/Ln Rgt 35
Aug 43 - Apr 45	14/Ln Rgt 1 = 1/Ln Rgt 353.

In FRANCE, P.W. had been stationed at URVILLE near CHERBOURG as an intercept operator taking Coastal Command W/T traffic in connection with U-boats, but knew nothing of the results obtained.

From FRANCE he went to the BALKANS and then to RUSSIA, where he had early experience as a Signalmaster at VIII FLK and as a FLIVO with a field div. With 9/Ln Rgt 35, he received instruction in D/F, W/T 'I' and fusion, working particularly on the W/T traffic of RUSSIAN long-range bombers (ADD) which operated against the L of C and GERMANY proper. In Jul 43, P.W. was appointed O.C. of of 14/Ln Regt 1 (later renamed 1/Ln Rgt 353). In addition to his Sig Int work which mainly concerned fusion and order of battle, P.W. performed the normal duties of coy comd, so that his knowledge of freq, call sign and code systems was somewhat restricted, al-

though he could give names of specialists in these branches. His efforts having been almost entirely directed to the RUSSIAN Air Force, he had but scanty knowledge of the Army Sig Int.

2. RUSSIAN AIR FORCE TFC.

a) GROUND TO GROUND. Most successful results were obtained from the tfc of the RAB's (ground org corresponding to a Flughafenbereich) to the BAO's or bns, of which there might be up to 18 in a RAB. Most of the 3-fig and 4-fig tfc was readable and gave details of airfield locations, units engaged, serviceability of aircraft, POL supplies etc. The flying org (corps - div - regt) employed mostly 5-fig cipher.

Freqs for ground to ground tfc ranged between 1800 and 5500 kcs and were allocated by numbers from a freq table with intervals of 25 kcs. PW stated that gps could be identified without a knowledge of the freq allocation system.

b) FIGHTERS. For wireless control of fighters the RUSSIANS evolved an org of main control stas with sub-stas in the forward areas. By D/F of the movements of the main stas, the Schwerpunkt of future ground attacks could be deduced, while concentrations of sub-stas would indicate the main point of attack by tks or flying columns.

R/T exclusively was used. Fighter-bombers and ground-strafers communicated only to base and the first sign of their presence would often come from the R/T of the fighter escort.

Freqs varied between 3600 and 4600 kcs and occasionally up to 4800 kcs. On the NORTH RUSSIAN front call-signs were built up from code-names for the type of aircraft (fighter, fighter-bomber or ground-strafer) followed by a number indicating the unit e.g. BATSCHKA 37 = 59 IAP (Fighter Rgt). Individual planes would distinguish themselves by adding another number e.g. BATSCHKA 37/15. Both code-names and numbers changed every ten days, but continuity was maintained by an index of personalities mentioned in R/T or gleaned from PW interrogations.

Tfc consisted of instructions from control stas to fmn leaders and from the latter to individual planes, reports of losses, damage to planes etc. Place-names were sometimes mentioned in clear but more often reference points were used. These together with standard orders were sent in 3-fig code.

For taking fighter tfc, the GERMANS org listening posts right forward. Close cooperation was est with their own fighters and air observation service. D/F combined with careful recording of place-names in clear and decoded reference points completed the picture.

c) BOMBERS. Operations were directed mostly from the Air Force Div but occasionally from Corps. There would be no tuning before the aircraft took off but once airborne they would contact the ground sta with something like "MAR de TD25 = QSA ? K. Further activity would come up when the rendez-vous was reached and course would be set for the target with occasional msgs in 3-fig code giving positions along the route. Once over the enemy lines, wireless silence would be enforced until the mission had been carried out. Indications of the target could be obtained from the bearings sent out by the ground sta and additional information was obtained from RUSSIAN Flak networks. On the return flight frequent requests were made for bearings.

Two freqs in the 1900 - 4500 kcs range were employed; the

ground sta always operating on the lower. Peak activity was observed between 2500 and 3600 kcs.

d) NAVAL AIR FORCE. Used wireless sparingly, both R/T and W/T. Indications of operations were obtained from tuning-in before take-off and from tfc of fighter escort. Recce planes would give R/T instructions to the torpedo-carrying aircraft and to the MTB's.

3. RUSSIAN CODES AND CIPHERS.

a) 2-Fig. Only used by forward troops, almost 100% readable.
b) 3-Fig. Slightly more secure and reciphered daily. 80% readable.
c) 4-Fig. Only 60 % readable.
d) 5-Fig. Unbreakable unless the same reciphering pad was used more than once.

PW had no experience of breaking but gave certain details on the construction of these codes. These appear in the "Tech Notes on Codes and Ciphers".

With 4-Fig and 5-Fig, indicators and serial numbers provided some guide to the fmn involved.

4. ORDER OF BATTLE.

The following summary of order of battle details given by PW may afford some idea of the RUSSIAN Air Force potential:-

Front	Fmn	No. of Air Force Divs.
1 BALTIC	3 Air Army	12
2 BALTIC	15 Air Army	14
1 WHITE RUSSIAN	16 Air Army	21
2 WHITE RUSSIAN	4 Air Army	16
3 WHITE RUSSIAN	1 Air Army	14
1 UKRAINIAN	2 Air Army	22

TECHNICAL NOTES ON RUSSIAN CODES AND CIPHERS FROM P.W. INTERROGATION 11 AUG 45

1. INTRODUCTION

From the details of Russian frequencies and call-signs given by the Ps.W., it had been hoped to produce a consolidated report, but experiences varied so much that it was considered preferable to record them in the individual interrogation reports. On codes and ciphers, however, a certain measure of agreement was reached; the results are summarised below.

2. TWO-FIGURE

The two-figure code consisted simply of a large square, built up of 100 smaller squares (10 x 10), containing the vocabulary (figures, letters, words or phrases). Messages were enciphered by reading off the co-ordinates of the small vocabulary squares in terms of two figures. The code was employed mainly by the forward troops, and presented very little difficulty to the breaker, although the figure co-ordinates of the small squares might be re-shuffled daily.

Information obtained from the code was usually of very short-term value. Hptm HOLETZKO, however, mentioned the traffic of the

47 Guards Recce Regt (47 GDR\P) as having provided valuable information on enemy OB and intentions.

3. THREE-FIGURE

A. Construction of code

Diagram 1 shows the code-book open at the first page. On the inside of the cover four figures are printed (3, 5, 2, and 7); one of these forms the first figure of all the three figure groups, according to which quarter of the vocabulary page the clear happens to be in. The second figure of the code-book is taken from the centre strip. This strip is removable, and can be used for each page of the book. The third figure of the 3-figure group represents the page number shown on the thumb index. The order for enciphering then is:-

i) Cover number.
ii) Line number.
iii) Page number.

Examples:- ATT\CK - 351.
BOMBER - 201.
COMPANY - 521.
DIRECTION - 711.

All the encipherments of the vocabulary on this page end in figure 1, on the following page with figure 4, and so on.

B, Re-ciphering

The basic vocabulary, in RUSSIAN alphabetical order, would remain constant. In the experience of Lt. ST\RKE, the figures were changed every ten days according to a re-ciphering table similar to that shown in Diagram 2. The new cover and page-numbers would be obtained by taking the figures in line (a) and writing them in, clockwise, from the top left-hand corner. Column (b) would be used to replace the top ten figures of the centre strip, and column (c), beginning from the bottom, would fill the lower half of the centre strip. For the next ten-day period, line (d) and columns (e) and (f) would be used, and so on.

C. Breaking

Ps.W. had little knowledge of breaking methods, apart from frequency counts, but they admitted that traffic was mostly readable. Any experienced code-breaker will realise the considerable possibilities.

4. FOUR-FIGURE

A. Construction of code

Diagram 3 shows the top of the basic sheet as described by Hptm HOLETZKO. In the full sheet, there would be ten figures in column (a), giving a total of 1,000 divisions. Vocabulary was scattered, although alphabetical in blocks. To encipher, the figures would be read off in the order column (a), lines (b) and (c), and column (d).

B. Re-ciphering

Hptm HOLETZKO stated that, with the RUSSIAN Air Force, a complete reshuffle of all the figures took place daily, the vocabulary remaining unchanged. Ltn. ST\RKE said that the Army operated a slide on column (d), sometimes for every message. The first 4-figure group in a message would form an indicator.

5. FIVE-FIGURE

With 5-figure, the RUSSIANS used a basic vocabulary (assuming the proportions of a dictionary) for converting clear-text into 5-figure groups, and a one-time re-ciphering sheet of 100 random 5-figure groups which, taken in order, were added to the basic 5-figure groups. The result was the cipher text as sent. A message-form block contained fifty sheets, each bearing the 5-figure number of the whole block. Fifty re-ciphering sheets, numbered 1 to 50, were issued in a sealed envelope which bore the same 5-figure number as the message block.

The following aids to recognition occurred in the message:-

a) A 5-figure group in the first five or so groups of the message would be the actual number of the message block. This would remain constant for 50 messages.
b) A further 5-figure group, usually in the first seven groups of the message but always after the block number, would contain, as its last two figures, the number of the re-ciphering sheet (1 to 50) used. The middle figure of this group indicated the formation level, e.g. '6' might be Corps forward to Div, '5' might be Div to Div.
c) The last 5-figure group of the message was its serial number, starting from 00001 and continuing indefinitely in spite of change of message block. Newcomers to formations would start at 00001.

e.g. 57816 24835 61284 96358 53984 23781
(Block number)

47627 00841
(6-formation level.
27-reciphering-sheet number) (Msg serial number)

6. CONCLUSION

Although Ps.W. were most helpful, it must be emphasized that none of them was a code-specialist. Neither did any of them speak RUSSIAN, so that questions of vocabulary could not be raised. It seemed that the 3 and 4 figure codes would not present much difficulty from the breaking point of view, provided other sources (W/T 'I', D/F etc) gave some indications of the type of traffic involved.